

INTRODUCCIÓN A LA FORENSIA DIGITAL

CUERPO DOCENTE

- Prof:
 - Einar Lanfranco (einar@info.unlp.edu.ar)
- JTPs:
 - Sandra Zilla (szilla@info.unlp.edu.ar)

HORARIOS:

- Teoría: Jueves 18:30 a 20:30 (híbrido)
- Plataforma Moodle a través de <https://catedras.info.unlp.edu.ar>

LA METODOLOGÍA:

- Desarrollo de un trabajo integrador
- Entrega de prácticas y actividades
- Evaluaciones parciales on-line: no necesariamente múltiple choice.
- CTF (Capture The Flag).
- Asistencia a clase opcional, excepto días de evaluación y exposición.
- Entrega Final del trabajo integrador con exposición

¿CÓMO APROBAR LA CURSADA?

- La materia estará dividida en prácticas entregables y una parte teórica evaluada con coloquios.
- Tanto las prácticas como los coloquios se aprueban con **nota mayor a 4**.
- Para aprobar la materia no debe haber ni prácticas ni coloquios desaprobados.
- La nota de la cursada está compuesta por el **60% de la nota práctica + 40% de la nota teórica**.
- La nota final será el promedio de la nota de la cursada con la nota del trabajo integrador.
- La cursada se aprueba con una nota final mayor o igual a 4.

¿CÓMO APROBAR LA CURSADA?

- Ejemplos:
 - Promedio Práctica: $(5+8+6+9+7+6)/6 = 6.8$
 - Promedio Teoría: $(7+6+9+9)/4 = 7.7$
- Nota Práctica: $6.8 * 0.6 = 4$
- Nota Teoría: $7.7 * 0.4 = 3.1$
- Nota Cursada = $4 + 3.1 = 7$
- Nota TP integrador = 8
- Nota final de cursada = $(7 + 8) / 2 = 7.5$

RÉGIMEN DE EXAMEN FINAL:

- La nota de final de la materia se compone de la nota de la cursada más un trabajo extra a desarrollar que consistirá en la automatización de algunas de las etapas de la forensia digital aplicado a ejercicios de CTF.
- Nota de final= Nota de final de cursada +- 2 (de acuerdo al desarrollo de la automatización).

CTF

- Un CTF es una competición que permite poner a prueba habilidades sobre hacking por medio de diferentes tipos de desafíos.
- Resolver cada uno de estos desafíos llegaremos a una **flag**, que suele ser una cadena de caracteres con un formato específico como **FLAG{W3lc0m3_t0_CTF}**.
- La flag permite confirmar a la plataforma de la competición que hemos sido capaces de resolver el reto y normalmente, va acompañada de una compensación con puntos.

CTF: TIPOS DE CTF

- **Jeopardy:** Retos de diferentes temáticas (Crypto, Web, Forense, Reversing, Exploiting...) donde se ganan puntos cuando son resuelto según el nivel de dificultad.
- **Attack-Defense:** Cada equipo tiene un servidor o una red de equipos con vulnerabilidades que deben de proteger mientras que intentan conseguir acceso al equipo contrario.
 - En este reto hay puntos de ataque y puntos de defensa.

CTF: IFD

- Utilizaremos una plataforma de CTF tipo Jeopardy y la competición será en grupos.
- Las prácticas estarán compuestas, en parte, por desafíos obligatorios del CTF.
- Además habrá desafíos extras con dificultades variadas, entre ellos desafíos creados por alumnos de años anteriores.

CTF: UNLP

- Tenemos un equipo de CTF llamado SYPER y compuesto de docentes y alumnos de la facultad.
- Competimos en CTF nacionales e internacionales.
 - <https://ctftime.org/team/2003>
 - <https://www.info.unlp.edu.ar/docentes-de-informatica-ganaron-el-ctf-de-la-ekoparty/>

SISTEMA SEGURO:

"El único sistema seguro es aquel que está apagado, desconectado, dentro de una caja fuerte de titanio, enterrado en un bunker de concreto, rodeado de gas tóxico y vigilado por guardias armados y muy bien pagados. Y aún así, no apostaría mi vida a que es seguro".

Gene Spafford - Analista virus Morris

http://en.wikipedia.org/wiki/Gene_Spafford

INSEGURIDAD INFORMÁTICA

- La inseguridad informática es el conjunto de riesgos a los cuales están expuestos los recursos informáticos.
- Estos riesgos son muchos y muy variados: **virus y gusanos, spyware, ransomware, malware, ataques de denegación de servicio, accesos no autorizados, modificación de los sistemas, robos de información, etc.**

PROGRAMACIÓN SEGURA

- La programación segura, es una parte importante de la seguridad informática, englobada dentro del ámbito de la prevención.
- Un programa seguro es aquel que no puede ser utilizado para realizar funciones distintas de las que ha sido diseñado.
- La programación segura es el conjunto de técnicas, normas y conocimientos que permiten crear programas cuyo uso no pueda ser vulnerado.

FUNCIONALIDAD Y SEGURIDAD

- Los programadores suelen conformarse con que su programa funcione, es decir satisfaga los requerimientos funcionales.
- Los fallos se corrigen luego, generalmente no se preveen.
- Programar de forma segura conlleva un mayor tiempo de desarrollo, contrario a cumplir los plazos de mercado.

FUNCIONALIDAD Y SEGURIDAD

- Los programadores son humanos, es prácticamente imposible no equivocarse.
- No existe una conciencia real sobre el problema de la seguridad.
- Los consumidores no se preocupan realmente de este tema y sí de que el programa satisfaga la funcionalidad demandada.

HASTA QUE ES TARDE....



- **Deface o defacement** manipular la página principal de un servidor web sin autorización, dejando algún tipo de mensaje en texto, imagen, vídeo...
- Puede ser de carácter reivindicativo político, lo que sería hacktivismo, para avergonzar a los responsables del sitio, o simplemente un graffiti al estilo "estuve aquí".

2013) MIT

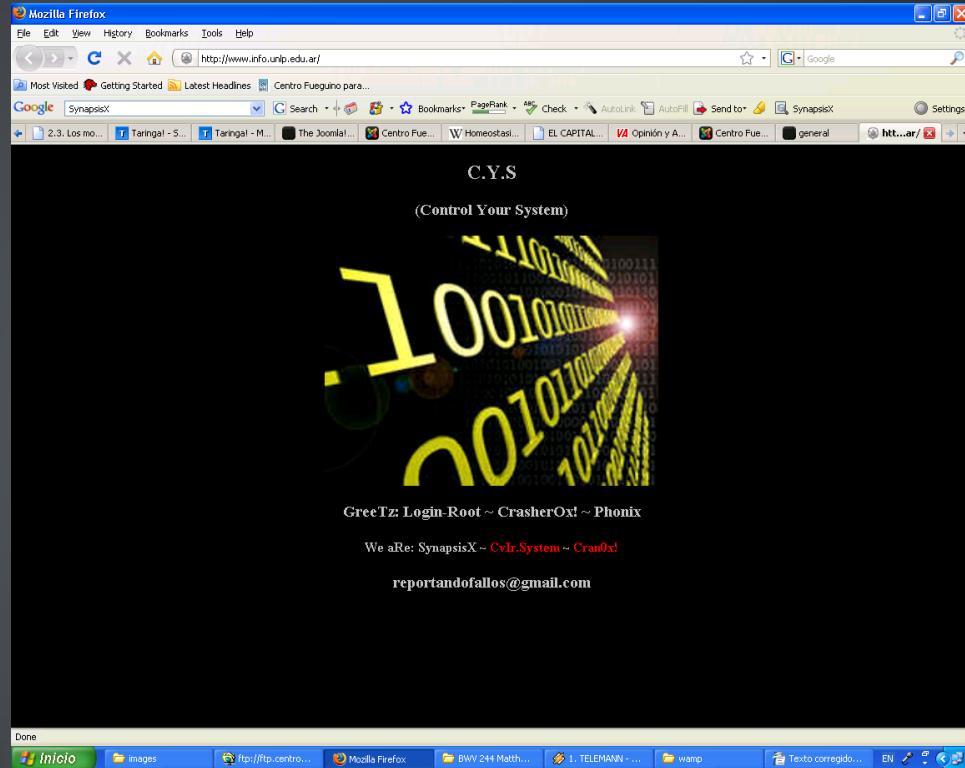
The screenshot shows a web browser window with the URL www.mit.edu in the address bar. The page content has been hacked, displaying a dark background with white text. At the top, it reads:
I used to think I was a pretty good person. I certainly didn't kill people, for example. But then Peter Singer pointed out that we were conscious and that eating them led them to be killed and that wasn't all that morally different from killing a person.
I became a vegetarian. Again I thought I was a pretty good person. But then Arianna Huffington told me that by driving my car, I was pouring toxic fumes into the air and sending money to foreign dictatorships. So I got a bike instead. But then I realized that even that was sown by children in foreign sweatshops.

R.I.P Aaron Swartz
Hacked by grand wizard of Lulzsec, Sabu

G O D B L E E S S A M E R I C A
D O W N W I T H A N O N Y M O U S

The rest of the page is heavily redacted with black text, obscuring further details of the hack.

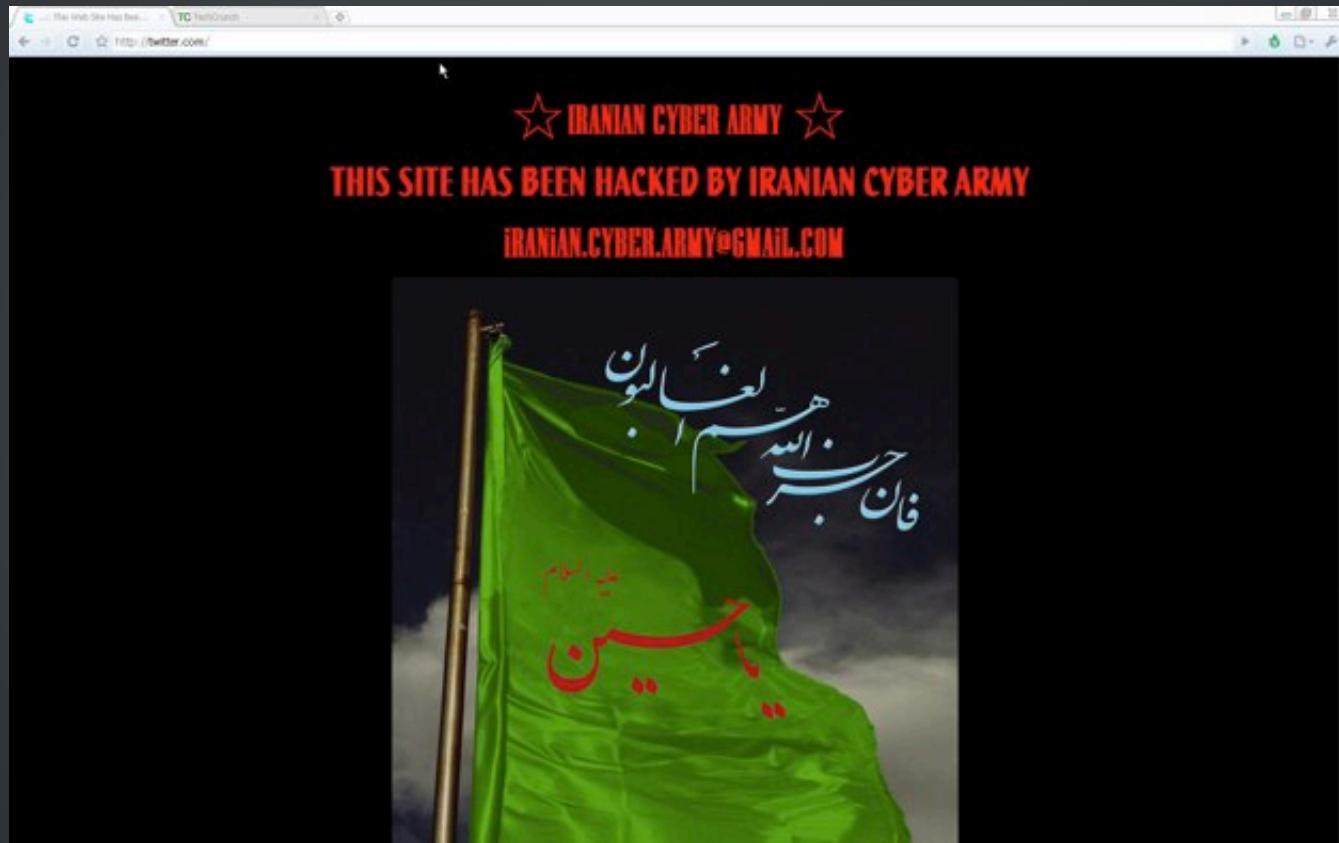
200X) INFO DEFACED



(2009) ESPN.COM - THE MAGICAL LAND OF THE UNICORN



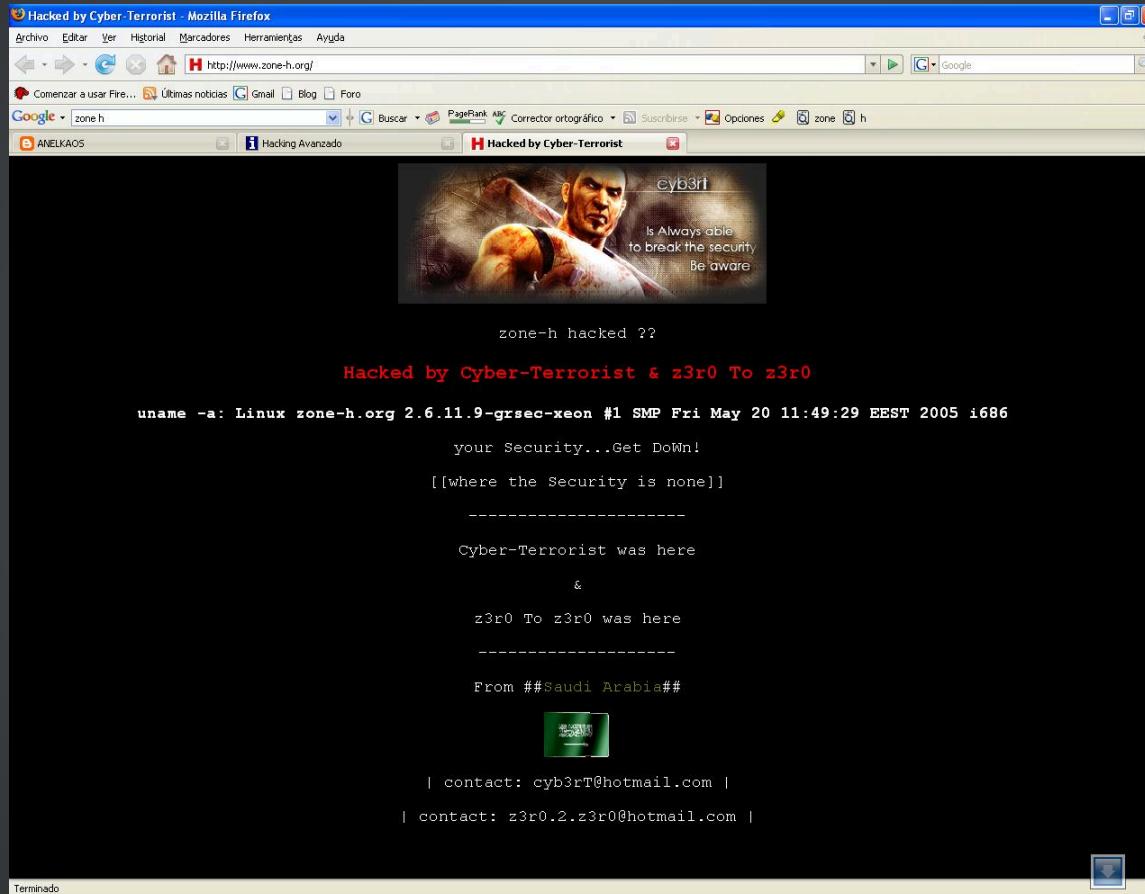
2009) TWITTER HACKED DEFACED BY "IRANIAN CYBER ARMY"



ZONE-H

- Zone-h es un directorio de sitios "defaceados"
- DEMO!

(2007) Y POR SUPUESTO...



EL MITO DEL AMBIENTE HOSTIL

- Son numerosos los documentos en los que se habla de ambientes hostiles, de ambientes confiables, o de entornos de bajo riesgo.
- La realidad es que **NO EXISTEN** los ambientes confiables.
- Todo ambiente confiable puede tornarse hostil, tanto en cuanto puede evolucionar ante determinadas circunstancias.
- Por ejemplo: Zoom en al año 2020

MYTH

- **Myth:** we are secure because we have a firewall (El de la foto aproximadamente u\$s 60.000)



MYTH

- Pero igual tiene passwords por defecto...

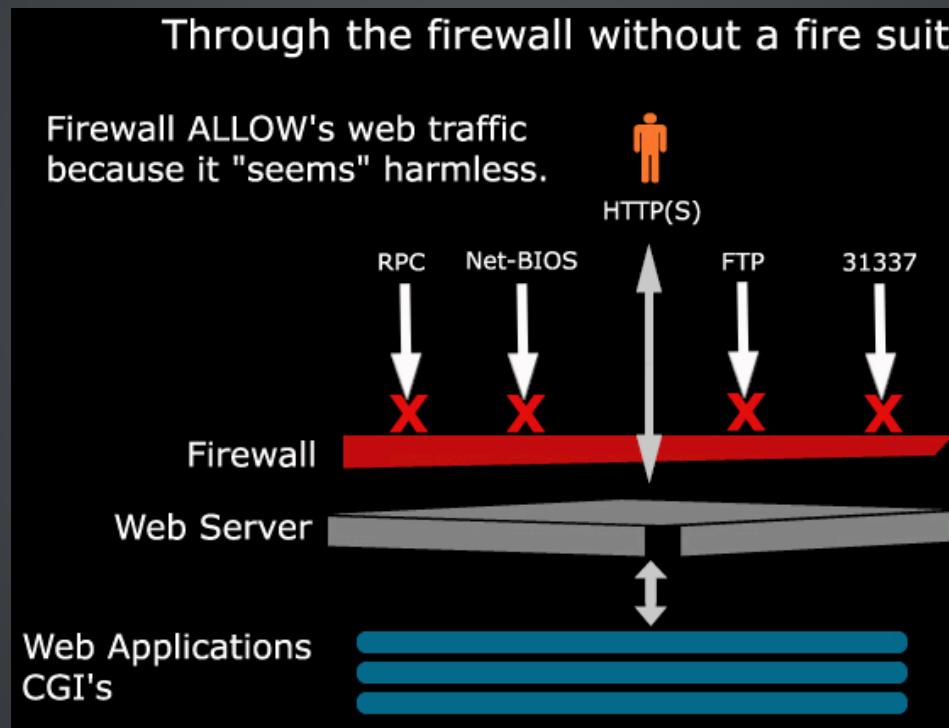
MYTH

- Pero igual tiene passwords por defecto...

Fortinet		
Model	Default Username	Default Password
Fortigate	admin	(none)
Fortigate	maintainer	bcpb+serial#
Fortigate	maintainer	admin

Fortinet Router Passwords - Port Forward
<https://portforward.com/router-password/fortinet.htm>

MYTH DEL FIREWALL: TIENEN QUE DEJAR A LAS APLICACIONES WEB FUNCIONAR

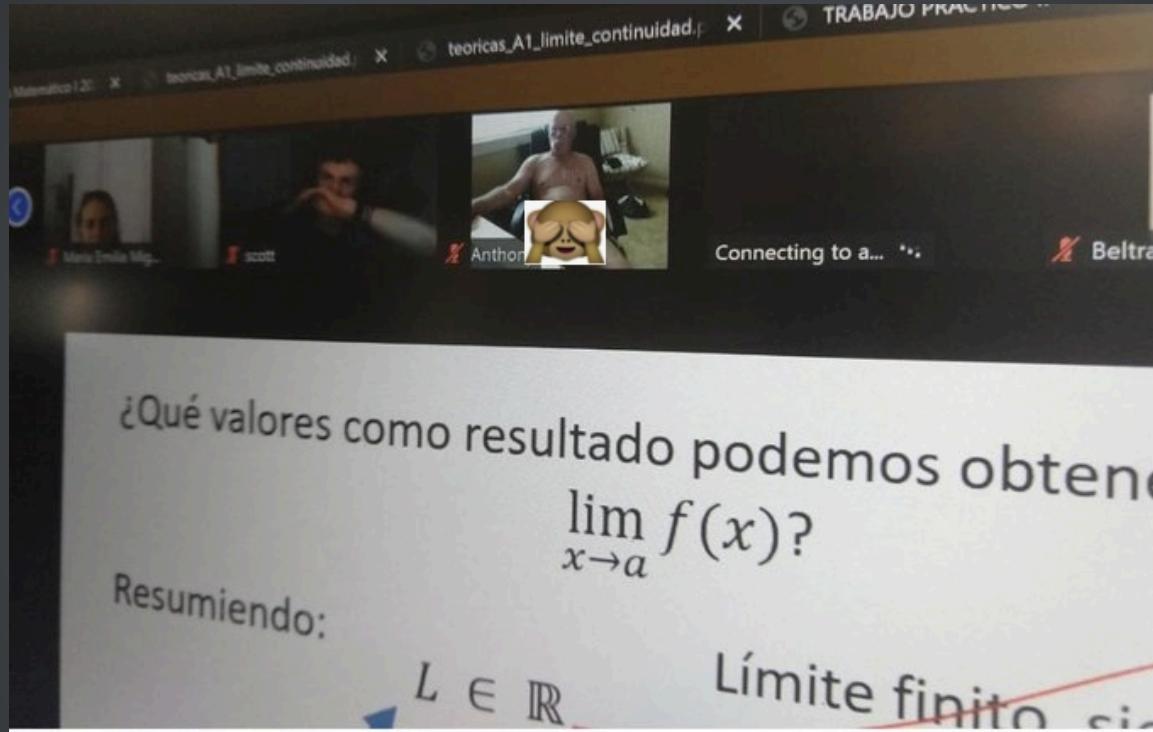


LA PROBLEMÁTICA

- Las aplicaciones web están disponibles y accesibles desde cualquier lugar del globo las 24 hs los 365 días del año!
- Porcentaje de sitios Vulnerables:
 - Según Acunetix +70%
 - Según Imperva +95%
- La explotación no requiere conocimientos: Kits de explotación

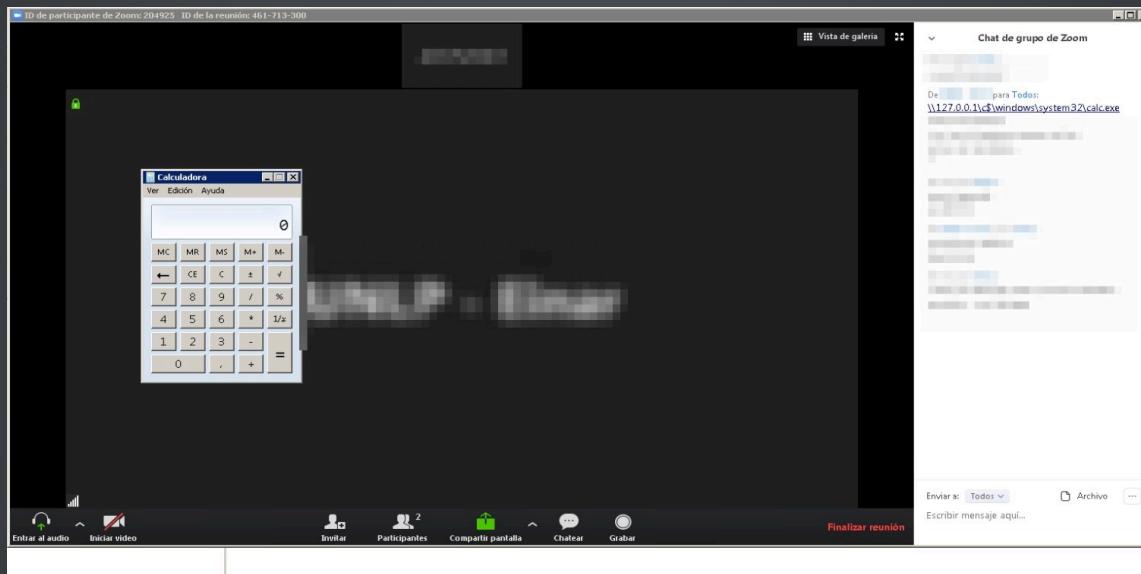
**¿ESTOS MITOS SON SOLO A NIVEL
DEPARTAMENTOS DE IT?**

ZOOM BOMBING O ZOOM LEAK



- Fuente:
https://twitter.com/gioacchin_/status/124552668319

UNC PATH INJECTION



Link

ZOOM DIPUTADO



- Fuente: <https://www.youtube.com/watch?v=faCYy7OGaJw>

CONCEPTOS BÁSICOS

- Una **vulnerabilidad** es una debilidad en un activo.
- Una **amenaza** es una violación potencial de la seguridad. Las amenazas sacan ventaja de las vulnerabilidades.
- Un **incidente de seguridad**, es un evento adverso que afecta los activos.
- Las amenazas sacan ventaja de las vulnerabilidades.

EJEMPLOS CONCEPTOS

- **Vulnerabilidad:** Ventana sin rejas.
- **Amenaza:** Que alguien pueda entrar a través de esa ventana.
- **Incidente:** Concreción de una amenaza, “un ladrón entró el martes a las 17hs por la ventana y se llevó el televisor”

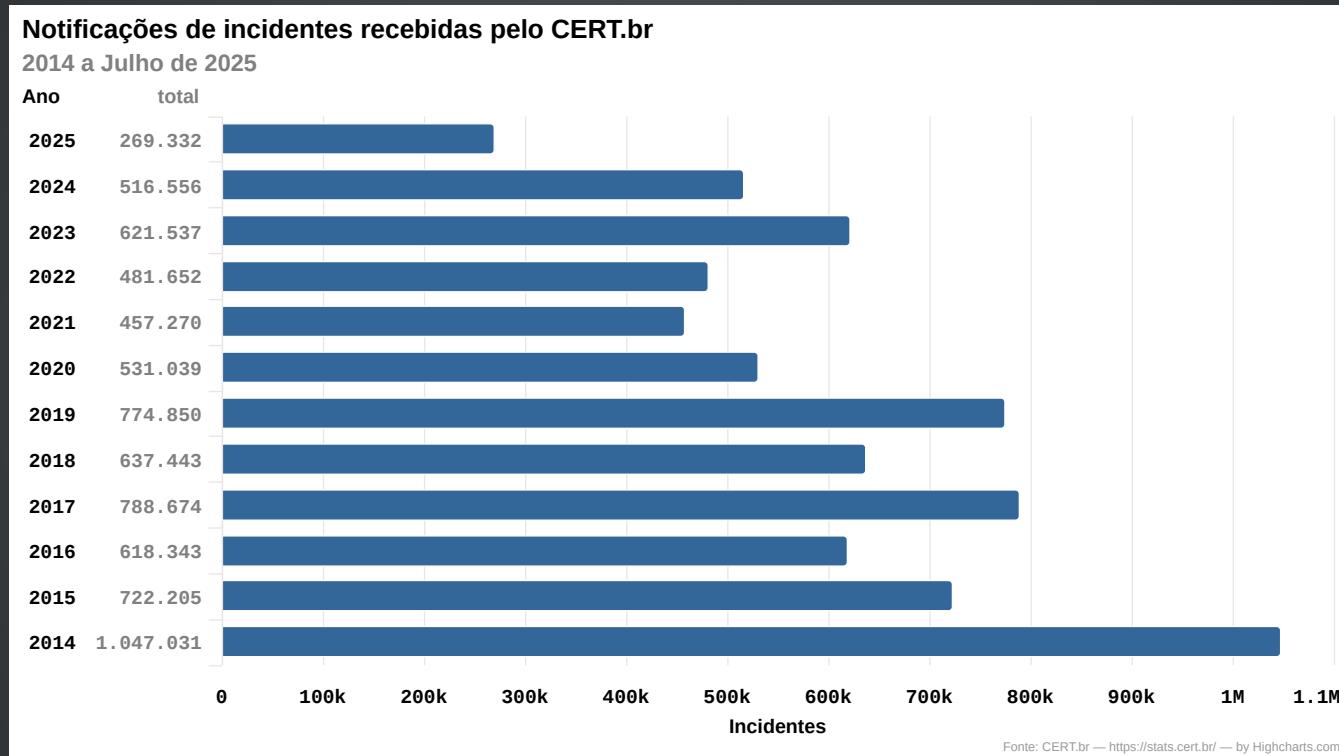
EJEMPLO APLICADO

- **Vulnerabilidad:** Un software que tenga acceso a posiciones de memoria según lo que se indique en el uso.
- **Amenaza:** Que alguien manipule el software para que lea información de esa posición al usuario.
- **Incidente:** Concreción de una amenaza, "que alguien utilice el software para leer la memoria del equipo donde se esta ejecutando"

EJEMPLO APLICADO

- **Vulnerabilidades:**
 - Falta de concientización del usuario
 - Falta de procedimientos de respuesta
 - Falta de uso de mecanismos de encriptación
- **Amenaza:**
 - Qué se comprometa la reputación de la organización a nivel local y del país a nivel regional
 - Que se filtren datos de acceso
 - Que se pierda la confidencialidad de los datos que maneja el ministerio
- **Incidente:**
 - El usuario recibe un correo adjunto y entrega sus contraseñas de acceso al Twitter y las cuentas de mail.
 - El atacante publica en la deep web la información del ministerio y sus agentes

REPORTE CERT.BR 2025



Link al reporte de incidentes cert.br

EXPLOITS

- Un exploit es un programa que se aprovecha de una vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.
- Un kit de exploit es una biblioteca de exploits, creada por diferentes personas cuya principal finalidad es agrupar el mayor número de exploits posibles, al menos los más relevantes y funcionales, de manera que cualquiera, ya sea investigador de seguridad o pirata informático, pueda utilizar el exploit que necesite fácilmente sin tener que pasar horas buscando su código en la red.
- Un exploit puede ser ejecutado por cualquiera, no se requiere mucho conocimiento para ejecutarlos.

CVE-2014-0160

- Conocido como HeartBleed
- Permitía recuperar 64Kb de memoria a partir de una vulnerabilidad en OpenSSL v 1.0.1
- la version 1.0.1 fue publicada en el 2012 y la vulnerabilidad fue explotada recien 2 años mas tarde en el 2014

Mark Loman @markloman · 7h
@yahoo your login servers are vulnerable for the OpenSSL #heartbleed attack, exposing usernames and plain passwords pic.twitter.com/v8kddiP0Yo

```
0070: 2D 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 - HTTP/1.1..Host
0080: 3A 20 6C 6F 67 69 6E 2E 79 61 68 6F 6F 2E 63 6F : login.yahoo.co
0090: 6D 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A m..Accept: */*..
00a0: 59 61 68 6F 6F 52 65 6D 6F 74 65 49 50 3A 20 31 YahooRemoteIP: 1
00b0: 34 39 2E 32 35 34 2E 35 [REDACTED] 0D 0A 0D 0A 49.254.5[REDACTED]...
00c0: 03 2D 67 5D EF 0C 27 2E 8C 10 27 A0 43 C5 45 6F ..-g)...'.C.Eo
00d0: C2 85 A3 BC 6E 65 3D 68 74 74 70 73 25 33 41 25 ...ne=https%3A%
00e0: 32 46 25 32 46 77 77 2E 79 61 68 6F 6F 2E 63 2F%2Fwww.yahoo.c
00f0: 6F 6D 25 32 46 26 2E 70 64 3D 66 70 63 74 78 5F om%2F&.pd=fpctx_
0100: 76 65 72 25 33 44 30 25 32 36 63 25 33 44 25 32 ver%3D0%26c%3D%2
0110: 36 69 76 74 25 33 44 25 32 36 73 67 25 33 44 26 6ivt%3D%26sg%3D&
0120: 2E 77 73 3D 31 26 2E 63 70 3D 30 26 6E 72 3D 30 .ws=1&.cp=0&nr=0
0130: 26 70 61 64 3D 36 26 61 61 64 3D 36 26 6C 6F 67 &pad=6&aad=6&log
0140: 69 6E 3D 70 69 65 72 72 65 69 [REDACTED] 26 in=pierre[REDACTED]&
0150: 70 61 73 73 77 64 3D 63 72 6F 6E 61 6C [REDACTED] passwd=cronal[REDACTED]
0160: [REDACTED] 26 2E 70 65 72 73 69 73 74 65 6E 74 3D [REDACTED] &.persistent=
```

Expand Reply Retweet Favorite More

CVE-2014-0160

HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



This page about "boards" user Erica requires
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
Meg (charles) sends this message: "

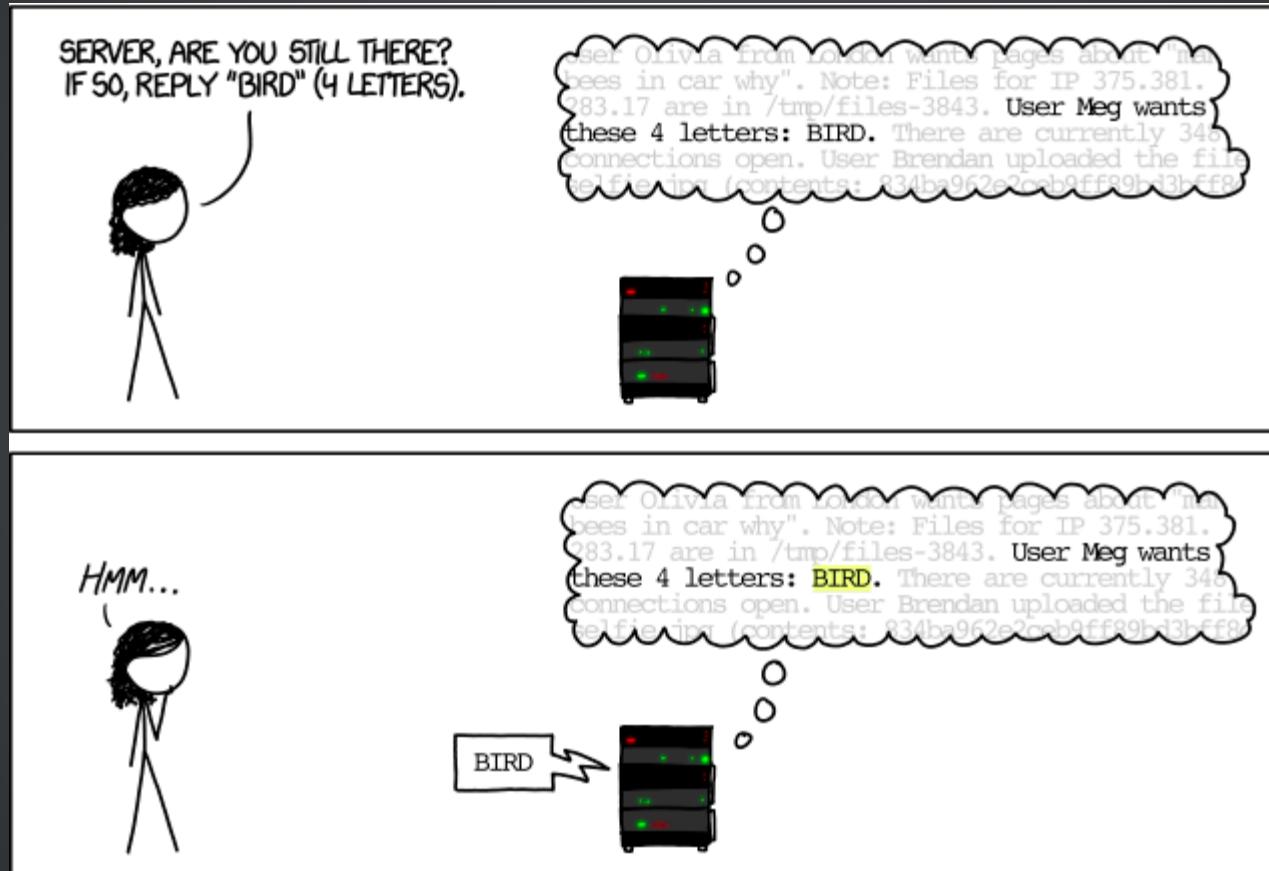


This page about "boards" user Erica requires
secure connection using key "4538538374224"
User Meg wants these 6 letters: POTATO. User
Ada wants pages about "irl games". Unlocking
secure records with master key 5130985733435
Meg (charles) sends this message: "

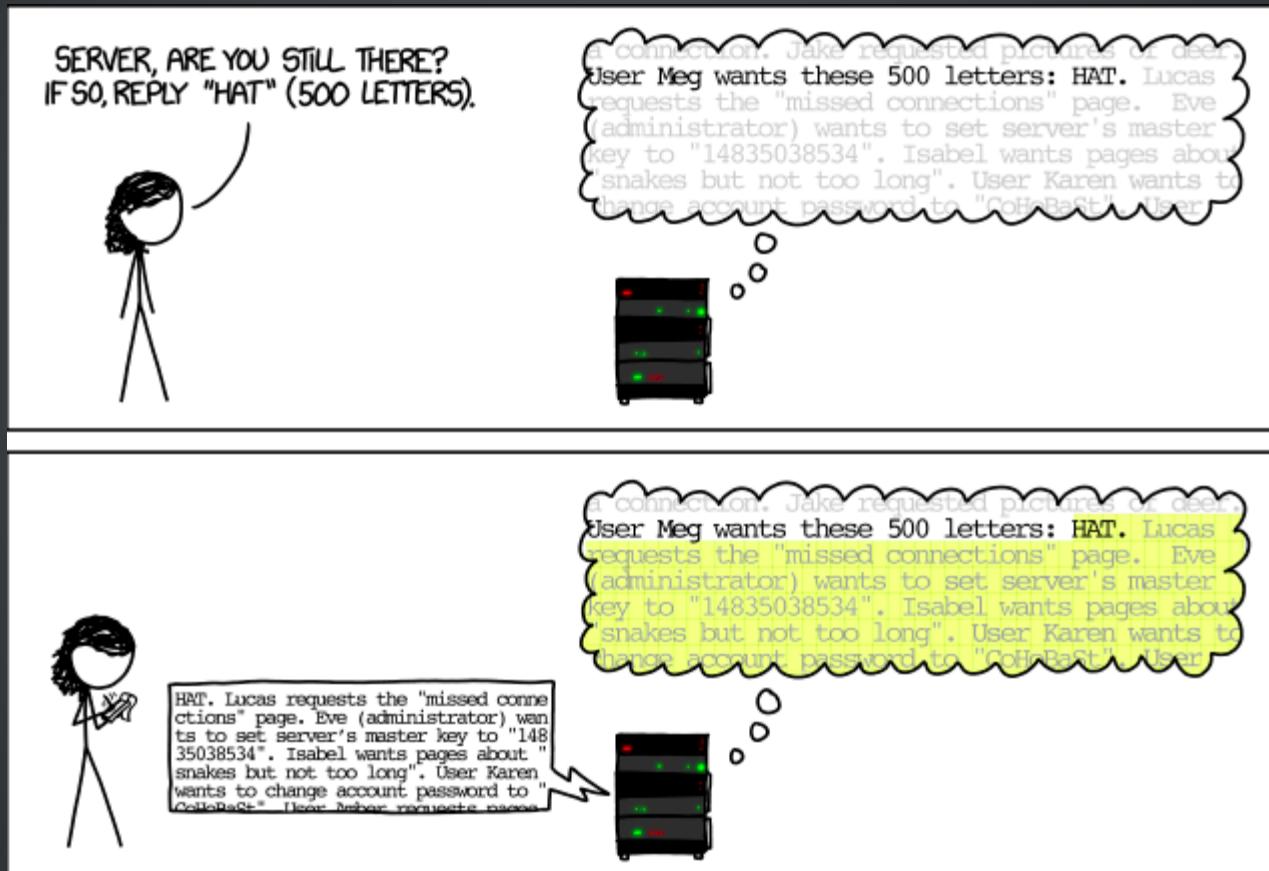
POTATO



CVE-2014-0160

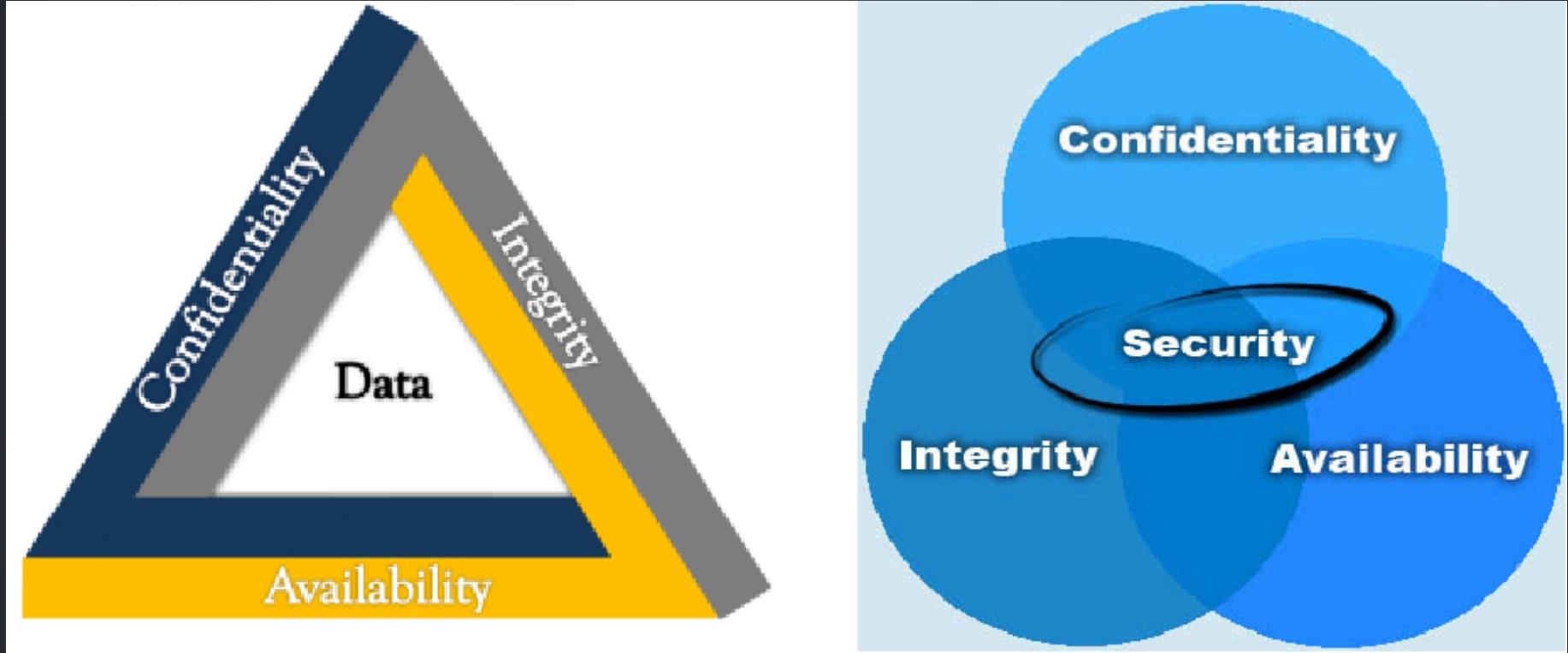


CVE-2014-0160



SEGURIDAD DE LA INFORMACIÓN

- La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la **confidencialidad, la disponibilidad e integridad** de datos.
- Estas propiedades suelen llamarse **Triangulo CIA** por su definición en inglés.



TRIÁNGULO CIA: CONFIDENCIALIDAD

- La **confidencialidad** es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados.
- Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

TRIÁNGULO CIA: INTEGRIDAD

- La **integridad** la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

TRIÁNGULO CIA: DISPONIBILIDAD

- La **disponibilidad** es la característica, calidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- Es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

¿DESDE DONDE ME ATACAN?



- <https://threatmap.checkpoint.com/ThreatPortal/livemap.html>

¿POR QUÉ?

Antes	Ahora
Por diversión	Crimen organizado
	Cyber-espionaje
Sin fines de lucro	Fines de lucro
El impacto en las organizaciones era menor	Afectar la imagen
Distribución masiva	Desarrollo focalizado
Destruir información o dejar inoperable el equipo	Utilizar los equipos para su beneficio (ej: DDoS, Zombies)

¿POR QUÉ?: PUERTO DE AMBERES

- En 2011, del importante puerto europeo de Amberes, misteriosamente comenzaron a desaparecer contenedores.

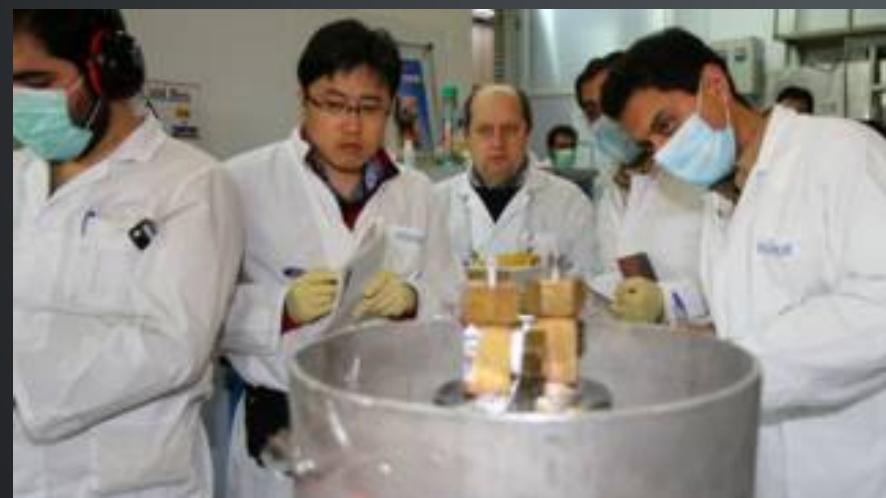


¿POR QUÉ?: PUERTO DE AMBERES

- los sistemas de seguridad habían sido hackeados por una organización criminal que comenzó a usar el puerto para introducir drogas en cargamentos que supuestamente eran plátanos provenientes de Sudamérica.
- <http://www.bbc.com/news/world-europe-24539417>
- <https://www.infobae.com/america/mexico/2018/11/02/narcos-y-hackers-como-funciona-esta-nueva-alianza-delictiva-que-crece-en-la-oscuridad/>

¿POR QUÉ?: STUTNEX

- **Stutnrex:** Malware que se detectó en 2010 en la nuclear de Natanz de Irán, se cree que destruyo 1000 máquinas centrifugadoras que se utilizan para enriquecer uranio.
- Se dice que la idea de EEUU e Israel era demorar el programa nuclear de Irán, ni energía ni armas.
- **Reporte de BBC**



STUTNEX EL ¿POR QUÉ?

- Según Symantec:
 1. Stuxnet penetró en la red mediante pens usb plantados
 2. El gusano se propagó a través de las computadoras
 3. Stuxnet reprogramó las centrifugadoras acelerándolas y enletenciéndolas
 4. Destrucción de las máquinas al girar muy rápido

¿POR QUÉ? CRYPTOJACKING



- Ejemplo 1: [12/2017 The guardian](#)
 - Miles de millones de visitantes de sitios de videos extraen criptomonedas sin saberlo mientras ven los sitios populares.
 - Openload, Streamango, Rapidvideo y OnlineVideoConverter supuestamente obligan a los usuarios a extraer criptomonedas Monero

¿POR QUÉ? CRYPTOJACKING



- Ejemplo2: [11/2/2018 - The Guardian](#)
 - En Inglaterra varios websites gubernamentales fueron infectados por un malware que forzó a los browser de los visitantes a minar criptomonedas.

CARBANAK

Carbanak: un robo de 1.000 millones de dólares Un ataque dirigido contra un banco

1. Infección



2. Obtención de inteligencia

Interceptación de las pantallas



3. Suplantación del empleado

3. Suplantación del empleado

Cómo robaron el dinero

Banca online

Dinero transferido a las cuentas de los ciberpiratas

Sistemas de pago electrónico

Dinero transferido a bancos en EE.UU. y China

Aumento de saldos en cuentas

Fondos adicionales extraídos mediante transacciones fraudulentas

Control de cajeros automáticos

Instrucciones para entregar efectivo en un momento predeterminado

Cientos de equipos infectados

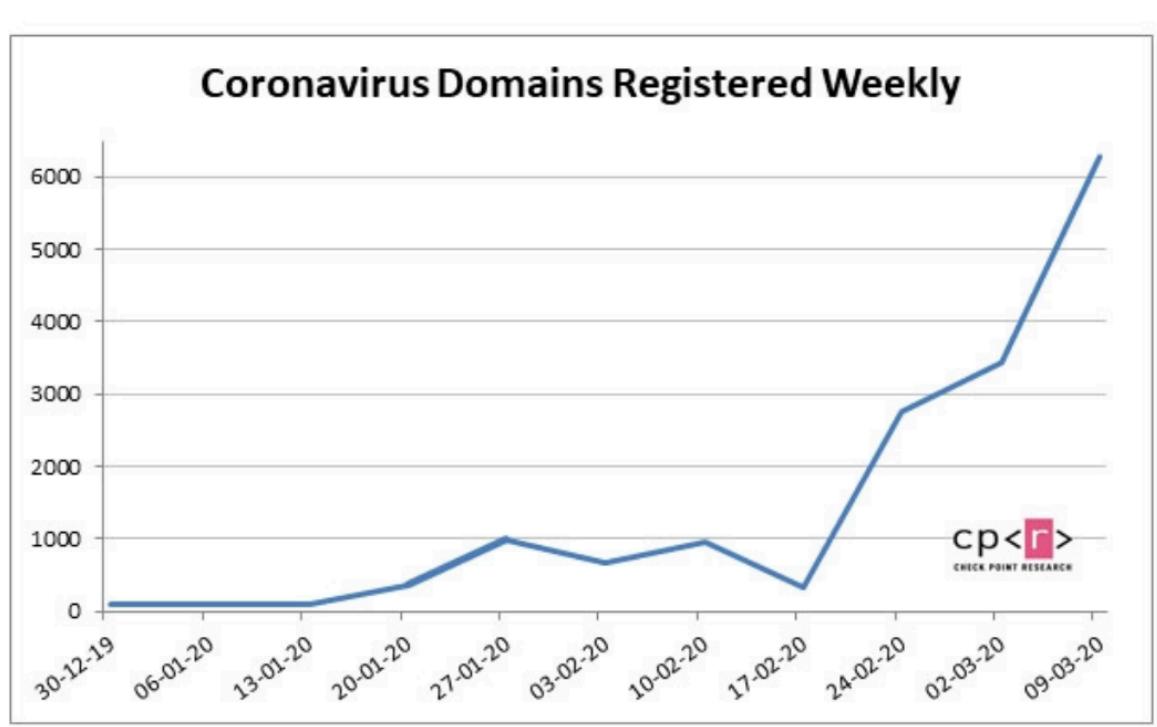
en busca del PC admin





Explicación Carbanak

CONSECUENCIAS DE LA PANDEMIA



- accorona[.]com
- alphacoronavirusvaccine[.]com
- anticoronaproducts[.]com
- beatingcorona[.]com
- beatingcoronavirus[.]com
- bestcorona[.]com
- betacoronavirusvaccine[.]com
- buycoronavirusfacemasks[.]com
- byebye-coronavirus[.]com
- cdc-coronavirus[.]com
- combatcorona[.]com
- contra-coronavirus[.]com
- corona-armored[.]com
- corona-crisis[.]com
- corona-emergency[.]com
- corona-explained[.]com
- corona-iran[.]com
- corona-ratgeber[.]com
- coronadatabase[.]com
- coronadeathpool[.]com
- coronadetect[.]com
- coronadetection[.]com

REAL LIFE DISPONIBILIDAD

CORPORATIVO

Ataques DDoS a Pymes cuesta entre 49 y 90 mdd anuales

Latinoamérica concentra el 15.6% de los ataques a nivel mundial; mientras que México registró 19,504 violaciones en 2016

Miércoles, 25 de octubre de 2017

Ransomware Cyberattack Information

Font Size: + - Share & Bookmark Feedback Print



RANSOMWARE CYBERATTACK INFORMATION-HUB

The City of Atlanta is committed to making sure that employees and the public are kept informed after a March 22 ransomware cyberattack affected multiple applications and client devices. A cross-functional team, including public and private sector partners, is working around-the-clock assessing what occurred and how best to protect our city from not just this attack, but others the city may face in the future.

While some customer applications are disabled, the City continues to operate and is open for business on behalf of its residents. City employees and residents are encouraged to visit this site regularly for updates.

- Ver

REAL LIFE DISPONIBILIDAD

Trains stations in Germany



REAL LIFE DISPONIBILIDAD

← Tweet



¿#Ransomware? || La Legislatura porteña sufrió un ciberataque.

Me niegan que sea un caso de ransom, pero el comunicado dice que hay máquinas encriptadas 🖥️🔒

Salvo que alguien esté encriptando por deporte, es raro. El comunicado oficial 👇📄

Comunicación: ciberataque en la Legislatura de la Ciudad

El domingo 11 de septiembre se detectó que parte del Sistema de la Legislatura de la Ciudad de Buenos Aires había recibido un ciberataque.

Inmediatamente se tomaron medidas para evaluar y controlar el daño. **Toda la labor parlamentaria en la Legislatura continuará su funcionamiento tomando los recaudos necesarios.**

Asimismo, ya se realizó una presentación judicial ante la Unidad Especializada en Delitos y Contravenciones Informáticas de la Ciudad de Buenos Aires.

¿Qué va a hacer la Legislatura frente a esta situación?

- Detectará la vulnerabilidad en nuestra infraestructura para poder mitigarla.
- Redactará un informe para evaluar el estado de situación. Abarca, por ejemplo, qué sistemas están encriptados, qué servidores, qué usuarios y qué máquinas.
- Restaurará todos los perfiles de accesos.
- Realizará un inventario de los servidores y máquinas que tenemos que restaurar para poder abordar todo en conjunto. De modo contrario, restaurar la situación podría demorar meses.

En simultáneo a lo expresado, **creamos un Comité de Crisis** integrado por referentes de diversas áreas de la Legislatura. Este Comité estará delineando un Plan de Acción, con acciones priorizadas, que permita volver al funcionamiento normal del sistema. Entre las acciones priorizadas se encuentra la de restaurar los sistemas involucrados en la labor parlamentaria.



Comunicado

Queremos informarles que los sistemas de PAMI han experimentado un ciberataque que ha afectado temporalmente el servicio. El ataque ha sido mitigado y toda la información de nuestros servidores se haya resguardada y protegida.

Asimismo, como parte del plan de contingencia, los sistemas se han suspendido y serán dados de alta progresivamente.

Turnos programados con médicos de cabecera y especialistas

Informamos a todos los médicos de cabecera, clínicas, sanatorios y hospitales del país que los turnos ya programados a la fecha deben ser atendidos con normalidad y se permitirá la transmisión cuando el sistema sea restablecido. Las consultas serán validadas aunque no se hayan transmitido en tiempo real.

REAL LIFE INTEGRIDAD

Le hackearon la cuenta de Twitter a Patricia Bullrich

Es la ministra de Seguridad de la Nación. Mirá los mensajes que dejaron.

Macri gato

49 1,3 K 569

Patricia Bullrich @PatoBullrich · 7 min
Soy una borracha inutil que le queda grande este cargo igual que al presidente @mauriciomacri el cargo de presidente.
35 532 280

Patricia Bullrich @PatoBullrich · 8 min
Hago de manera oficial mi renuncia como ministra de seguridad.

Los tuits en la cuenta oficial de la ministra Patricia Bullrich. (Twitter)

Sabina Frederic
674 Tweets



Sabina Frederic
@SabinaFrederic
Antropóloga Social Docente e Investigadora UNQ y CONICET. Ministra de Seguridad de la Nación Argentina.
Buenos Aires, Argentina conicet.academia.edu/SabinaFrederic
Se unió el diciembre de 2010
518 Siguiendo 1.490 seguidores
Followed by El Cohete a la Luna, CELS, and 4 others you follow

Tweets **Tweets y respuestas** **Multimedia** **Me gusta**

Sabina Frederic @SabinaFrederic · 21min
Encontramos cajas de vino en la oficina de Bullrich, las vamos a sortear a nuestros seguidores, muy atentos
64 171 409

Sabina Frederic @SabinaFrederic · 30min
Un saludo al compañero Lázaro Baez pronto le daremos el cargo que se merece dentro del ministerio.
9 53 60

Sabina Frederic @SabinaFrederic · 37min
macri gato
18 46 57

Sabina Frederic @SabinaFrederic · 41min
Quiero agradecer a javier smaldone (@mis2centavos) por proveernos las contraseñas de la nueva ministra de seguridad xd
10 38 42

Cristina Kirchner @cfkresponde · 4 may.
La UNASUR tal vez no tenga el backstage de Naciones Unidas ni tampoco el marketing de Naciones Unidas pero sirve
1 2 ...

MARIANO SUAREZ @REVRAH · 4 may.
@cfkresponde CONSULTA.....gracias divina..... en la cárcel usarás ropa de fajina o te vestirás algún diseñador????
...
Cristina Kirchner @cfkresponde
@REVRAH Habla de ropa porque debe enviar mi buen porte
17:18 - 4 may. 2016
...
Item 4 of 4

REAL LIFE CONFIDENCIALIDAD

2018

Under Armour/MyFitnessPal

Roughly 150 million users of the MyFitnessPal app owned by Under Armour have had their personal details leaked in a data breach including usernames, email addresses and passwords.

In a written statement issued on 29 March, Under Armour said that it became aware of the breach on 25 March, though it actually occurred in late February 2018.

FedEx

A subsidiary of delivery and logistics multinational FedEx has stored extremely sensitive customer data on an open Amazon S3 bucket, essentially making all the information public.

The tranche of data was discovered by Kromtech security researchers on 5 February. The culprit looks like it was a company called Bongo International LLC, a package-forwarding business set up to make buying American goods easier for global customers, which was bought by FedEx in 2014.

It included thousands of scanned documents for citizens in America and globally – with passports, driving licences and security IDs all open for access in the bucket, as well as home addresses, postal codes and phone numbers.

2/5/17 · LAGORRALEAKS



- 40 megas ~ 215 archivos con información del Departamento de Inteligencia contra el Crimen Organizado de la Policía Federal.
- Incluyendo: declaraciones de testigos, sumarios, desgrabaciones del 911, causas de pedofilia, de narcotráfico, registros telefónicos, fotografías

12/8/19 - LAGORRALEAKS2



Prefectura Naval Arg ✅ @PrefecturaNaval · 1min
Gracias @PatoBullrich por el ginebral pegó re piola

2

6

5



Prefectura Naval Arg ✅ @PrefecturaNaval · 2min
LaGorraLeaks
Datos personales de todos los policías, escuchas, documentos confidenciales, etc.

lagorraleaks.co.nf

...wtwbchpkI5lgca53htfvf2i7umvuidid.onion
...wtwbchpkI5lgca53htfvf2i7umvuidid.onion/leak
...bchpkI5lgca53htfvf2i7umvuidid.onion.sh
...chpkI5lgca53htfvf2i7umvuidid.onion.pet
twitter.com/lagorraleaks

3

3

7



#LaGorraLeaks2.0 @lagorraleaks · 12h

Contenido:

- Escuchas Telefónicas.
- Documentos confidenciales.
- Información COMPLETA de cada uno de los agentes de la PFA Y POLICÍA DE LA CIUDAD y sus familiares.
- Documentación Escaneada.
- Copias de seguridad de Emails (PFA)

Y muchas cosas mas.

3

1

3

Tweet fijado



#LaGorraLeaks2.0 @lagorraleaks · 5h
Oficialmente hago publico #LaGorraLeaks2.0.

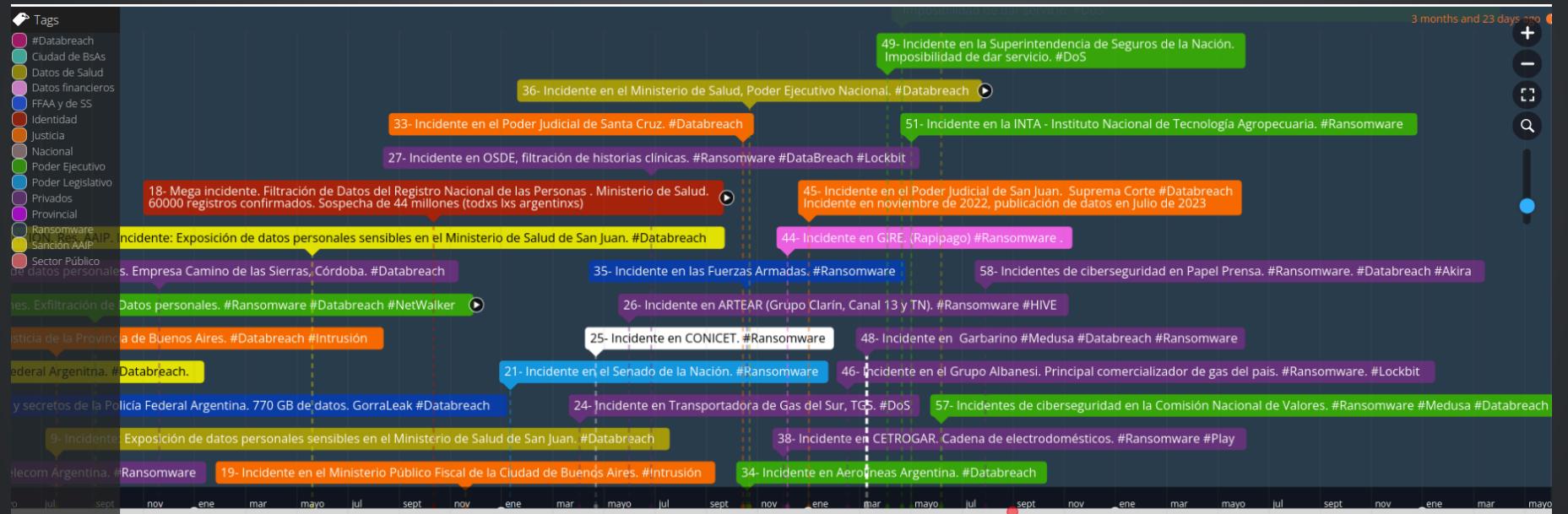
700 GB de información de la PFA Y POLICÍA DE LA CIUDAD.



- 700GB de información!!!

NADA TAN TRISTE COMO LA REALIDAD

- URL: <https://time.graphics/es/line/630567>



REAL LIFE TODO MEZCLADO

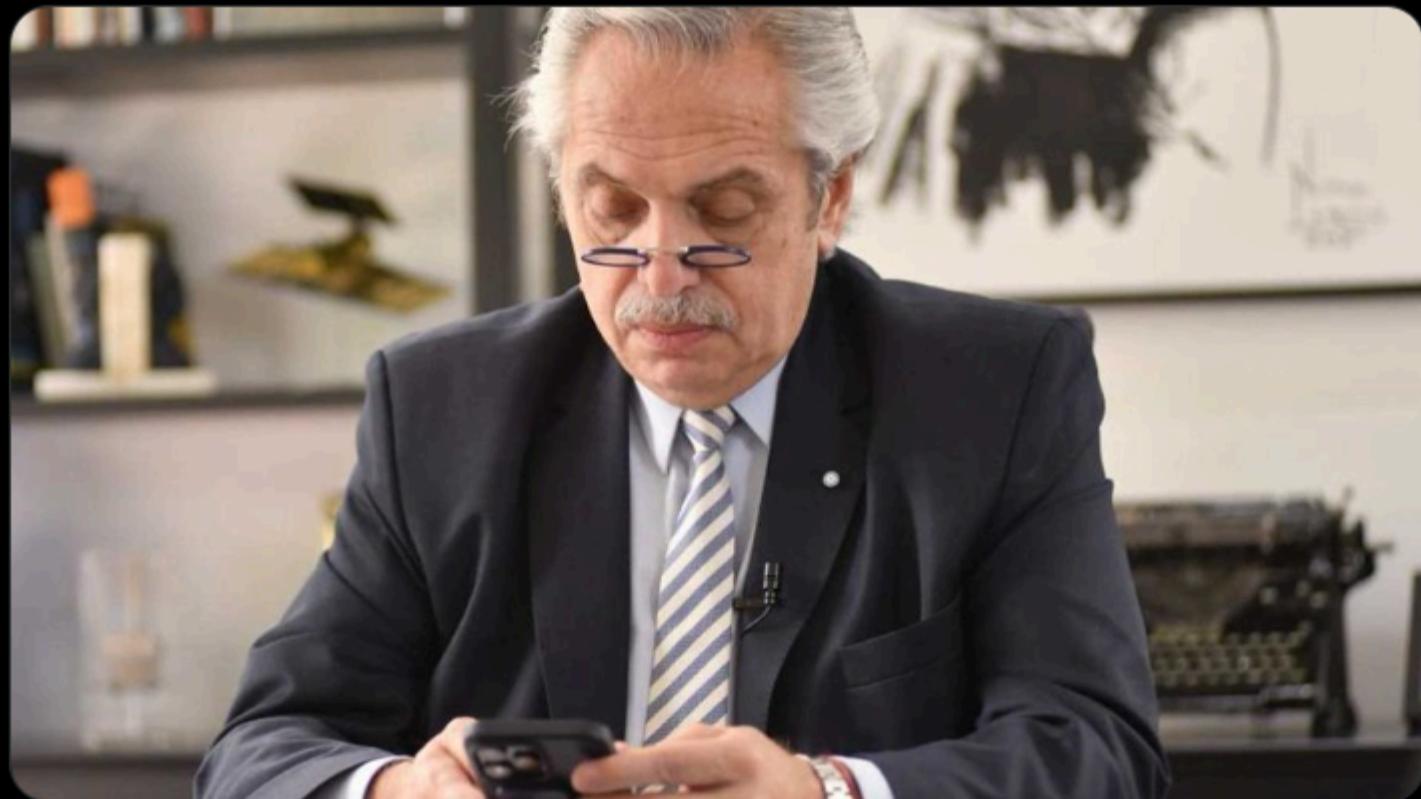
- Fraude Seguros (María Cantero, histórica secretaria Fernández, casada con Héctor Martínez Sosa)
- Chats relacionados (María Cantero - Yañez)
- Consulta a involucrados (Ercolini - Yañez)
- Nueva denuncia (Yañez al hacerse pública las conversaciones, le cae a Ercolini)
- Falta de cumplimiento (Fernandez hostiga Yañez, Ercolini secuestra equipamiento Fernandez)

PARALELAMENTE



CN24 NOTICIAS
@CN24NOTICIAS

#Justicia | #AlbertoFernández por medio de su abogada hizo una presentación ante el juez Julián Ercolini. Pidió a la Justicia que le devuelva sus teléfonos, que se prohíba la difusión de sus videos "íntimos" en medios y redes sociales y todo lo que secuestraron en su departamento



Y CUANDO CAMBIAMOS DE GOBIERNO

A la investigación por las coimas ahora se suman grabaciones que preocupan a la Rosada

Allanamientos, sospechas y encima nuevos audios

La justicia allanó la droguería involucrada pero hasta anoche se resistía a entregar la información requerida. La policía estuvo en la Andis y retiró documentación y computadoras.



Por **Irina Hauser**



INTRODUCCIÓN A LA FORENSIA DIGITAL

- El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad.
- Puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un usuario o intruso en los sistemas afectados por un evento de seguridad.

INTRODUCCIÓN A LA FORENSIA DIGITAL

- El análisis forense en un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad.
- Puede determinar quién, desde dónde, cómo, cuándo y qué acciones ha llevado a cabo un usuario o intruso en los sistemas afectados por un evento de seguridad.

IFD: EL PROCESO FORENSE

- La naturaleza de la evidencia digital es tal que esta posee desafíos para su admisibilidad en procesos legales.
- Para hacer frente a estos desafíos, hay que seguir procesos forenses adecuados.
- Estos procesos se componen básicamente de 4 fases:
 1. Recolección
 2. Examinación/Extracción.
 3. Análisis.
 4. Reporte.